Name: _____ Datum: _____ Punkte: _____

WireGuard vs. OpenVPN Arbeitsblatt

Vergleich der Protokolle WireGuard und OpenVPN, ihrer Codebasisgröße, Geschwindigkeit und kryptografischen Standards

VPN-LERNÜBERSICHT

LERNENDE
STUDIERENDENSTATUS
Lernpfad Netzwerkverteidigung

SICHER
VERBINDUNGSSTATUS
Abschirmung von Datenpaketen

AKTIV
SCHUTZ VOR LECKS
Schutz vor DNS- und IPv6-Leaks

Willkommen! Dieses Aktivitätspaket führt Sie durch die Grundprinzipien virtueller privater Netzwerke (VPNs). Sie erfahren, wie verschlüsselte Tunnel Ihre Daten schützen, wie Netzwerkprotokolle funktionieren und wie man Datenlecks bei der Privatsphäre erkennt und eindämmt.

KONTROLLPUNKTE DES ARBEITSBLATTS

- [ ] **Teil 1-4: VPN-Konzepte und -Protokolle beherrschen.**
- [ ] **Teil 5-7: Kreuzworträtsel und Suchsel lösen.**
- [ ] **Teil 8-9: Fallstudien und Chiffre-Aufgabe lösen.**
- [ ] **Teil 10: Seiten mit grundlegenden und fortgeschrittenen häufigen Fragen durchgehen.**
- [ ] **Teil 11: 10 interessante Fakten aus der Praxis entdecken.**
- [ ] **Bonus: Herausforderung Schnell denken.**

VPN-Leitfaden von VPN.com öffnen

URL: https://www.vpn.com/de/vpn/

Ihr Lernfahrplan: VPN

- Vergleichen Sie die Komplexität der Codebasis und die Prüfgeschwindigkeit der Protokolle.
- Analysieren Sie die Leistungsgewinne durch die Ausführung im Kernel-Space.
- Stellen Sie die Chiffren von OpenSSL der modernen Kryptografie von WireGuard gegenüber.
- Paare aus öffentlichem und privatem Schlüssel für den Handshake zwischen Peers einrichten.
- VPN-Verkehr über TCP- und UDP-Firewall-Ports leiten.

ANLEITUNG ZUM ARBEITSBLATT PROTOKOLLVERGLEICH

Beantworten Sie die Auswahlaufgaben und Richtig/Falsch-Fragen, vervollständigen Sie die Lückensätze mithilfe der Wortliste, ordnen Sie die Definitionen zu und lösen Sie das Kreuzworträtsel und das Suchsel. Wenden Sie Ihr Wissen in folgenden Bereichen an: Prüfung moderner Protokolle. Zum Schluss folgt die Bonusaufgabe Schnell denken.

WIREGUARD VS. OPENVPN (EINFÜHRUNG)

Bei der Wahl eines VPN-Protokolls muss man Geschwindigkeit und Konfigurationsmöglichkeiten gegeneinander abwägen. OpenVPN ist seit Jahrzehnten der Standard und bietet flexible Konfiguration über TCP/UDP. WireGuard ist ein moderner Ersatz, der direkt im Kernel-Space läuft und nur 4,000 Codezeilen umfasst. Das Verständnis der Unterschiede zwischen den Protokollen ist entscheidend, um Ihre sicheren Netzwerke zu optimieren.

LESEN SIE JEDEN KONTROLLPUNKT SORGFÄLTIG UND WÄHLEN ODER SCHREIBEN SIE DIE RICHTIGE ANTWORT.

Kontrollpunkt 1: Auswahlaufgaben

1 **1. Wie groß ist die Codebasis des WireGuard-Protokolls ungefähr?**

- A. Etwa 70,000 Zeilen
- B. Über 100.000 Zeilen
- C. Weniger als 1.000 Zeilen
- D. Rund 4,000 Zeilen

2 **2. In welchem Bereich des Betriebssystems läuft WireGuard?**

- A. User-Space
- B. Kernelbereich
- C. Anwendungsbereich
- D. Virtueller Raum

3 **3. Auf welche Kryptografiebibliothek stützt sich OpenVPN hauptsächlich?**

- A. ChaCha20-Poly1305
- B. Kryptografiebibliothek OpenSSL
- C. Noise Protocol Framework
- D. DES-Kodierung im Klartext

4 **4. Was ist ein wesentlicher Leistungsvorteil von WireGuard gegenüber OpenVPN?**

- A. Schnellere Verbindungs-Handshakes und geringere Latenz
- B. Umgehen der Notwendigkeit öffentlicher IP-Adressen
- C. Integrierte native Unterstützung für veraltete Einwahlverbindungen
- D. Kein zusätzlicher Akkuverbrauch auf Mobilgeräten

5 **5. Wie authentifiziert WireGuard Peer-Verbindungen?**

- A. Durch Austausch normaler Benutzerpasswörter
- B. Durch Überprüfen von Zertifikaten der Domainregistrierung
- C. Durch Verwenden statischer Paare aus öffentlichem und privatem Schlüssel
- D. Durch Prüfung von Hardware-Seriennummern

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Die kompakte Codebasis von WireGuard lässt sich deutlich leichter prüfen.

○ Richtig ○ Falsch

7 Frage 7

7. OpenVPN ist im Allgemeinen schneller als WireGuard, weil es im Kernel-Space läuft.

○ Richtig ○ Falsch

8 Frage 8

8. OpenVPN ist sehr flexibel konfigurierbar und unterstützt sowohl UDP als auch TCP.

○ Richtig ○ Falsch

9 Frage 9

9. WireGuard nutzt moderne Kryptografie wie ChaCha20 für eine schnelle Paketverschlüsselung.

○ Richtig ○ Falsch

10 Frage 10

10. WireGuard erfordert zur Authentifizierung komplexe Konfigurationen mit Zertifizierungsstellen.

○ Richtig ○ Falsch

Kontrollpunkt 3: Schlüsselbegriffe einsetzen

Lesen Sie jeden der folgenden Sätze und füllen Sie die Lücke mit dem richtigen Begriff aus der Wortliste.

1. Das moderne Protokoll _____ arbeitet direkt im Kernel des Betriebssystems.

2. Das ältere Protokoll _____ stützt sich auf die Kryptobibliothek OpenSSL.

3. Die Ausführung von Code im _____ verringert den Overhead durch Kontextwechsel.

4. OpenVPN läuft im _____ und leitet Pakete über virtuelle Schnittstellen.

5. Zur Identifizierung der Verbindungspartner nutzt WireGuard ein _____ aus öffentlichem und privatem Schlüssel.

6. Eine kleine Codebasis verbessert die sicherheitstechnische _____ der Software.

WORTSCHATZ-WORTBANK

KERNEL SPACE | OPENSSL | OPENVPN | PRÜFBARKEIT | SCHLÜSSELPAAR | TCP/UDP | USER SPACE | WIREGUARD

Schreiben Sie Ihre Antworten hier:

1.
2.
3.
4.
5.
6.

Kontrollpunkt 4: Zuordnung von Netzwerk-Begriffen

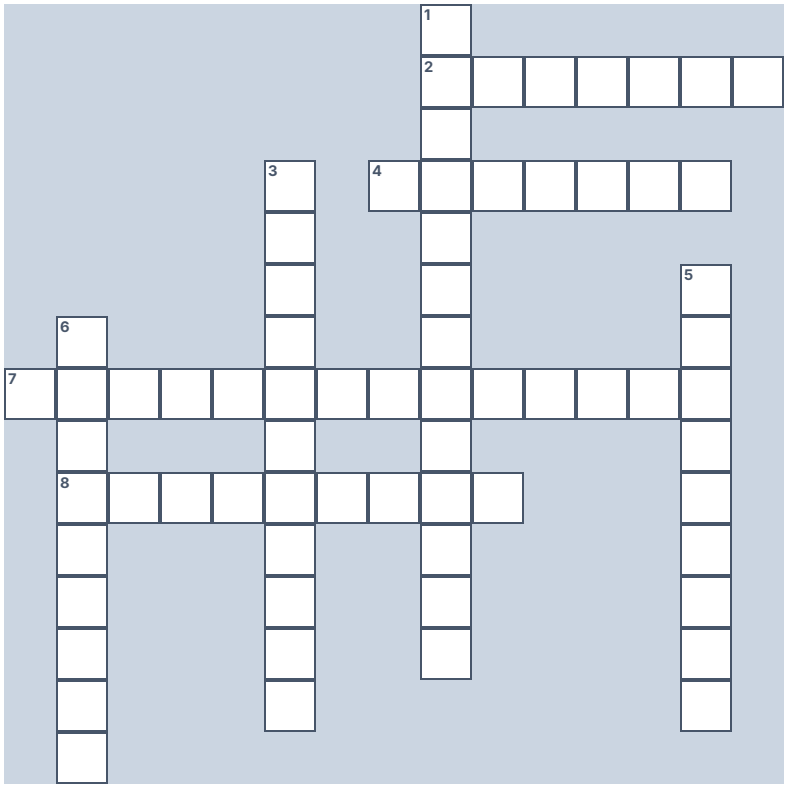
DEFINITIONEN ZUORDNEN

Ordnen Sie jeden Fachbegriff links der richtigen Definition rechts zu, indem Sie den passenden Buchstaben (A–H) in das ausfüllbare Eingabefeld schreiben.

☐	1. WireGuard	A	Ausführungsbereich, in dem OpenVPN läuft und zusätzlichen Aufwand durch Kontextwechsel verursacht.
☐	2. OpenVPN	B	Die kompakte Größe der WireGuard-Codebasis, die sie deutlich leichter überprüfbar macht.
☐	3. Kernel-Space	C	Kryptografische Bibliothek, auf die OpenVPN für Chiffre-Algorithmen zurückgreift.
☐	4. User-Space	D	Von OpenVPN unterstützte Transportprotokolle; WireGuard selbst läuft nur über UDP.
☐	5. 4.000 Zeilen	E	Ausführungsbereich des Betriebssystems, in dem WireGuard für mehr Geschwindigkeit läuft.
☐	6. OpenSSL	F	Asymmetrische Schlüssel, mit denen WireGuard Peer-Verbindungen überprüft.
☐	7. Schlüsselpaar	G	Modernes VPN-Protokoll, ausgelegt auf hohe Geschwindigkeit und einfache Code-Prüfung.
☐	8. TCP/UDP	H	Robustes älteres Protokoll mit einer großen, komplexen Codebasis.

Kontrollpunkt 5: Kreuzworträtsel

Lösen Sie das Kreuzworträtsel, indem Sie Buchstaben in die aktiven weißen Felder eingeben. Die Zahlen entsprechen den Hinweisen unten.



WAAGERECHT

2. Kryptografische Bibliothek, auf deren Chiffrier-Algorithmen OpenVPN angewiesen ist (7)

4. Robustes, älteres Protokoll mit großer, komplexer Konfigurations-Codebasis (7)

7. Asymmetrische Token, mit denen WireGuard Verbindungspartner verifiziert (14)

8. Ausführungsbereich, in dem OpenVPN läuft, was Overhead durch Kontextwechsel verursacht (9)

SENKRECHT

1. Geringe Größe der WireGuard-Codebasis, die die Prüfung deutlich erleichtert (13)

3. Ausführungsbereich des Betriebssystems, in dem WireGuard für mehr Geschwindigkeit läuft (11)

5. Modernes VPN-Protokoll für hohe Geschwindigkeit und einfache Code-Prüfung (9)

6. Transportprotokolle, die OpenVPN unterstützt; WireGuard selbst läuft nur über eines davon (9)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

Nutzer von Screenreadern und Tastatur können die Kreuzworträtsel-Antworten direkt in die Textfelder unten eingeben.

WAAGERECHT

2 waagerecht: Kryptografische Bibliothek, auf deren Chiffrier-Algorithmen OpenVPN angewiesen ist (7 Buchstaben):

4 waagerecht: Robustes, älteres Protokoll mit großer, komplexer Konfigurations-Codebasis (7 Buchstaben):

7 waagerecht: Asymmetrische Token, mit denen WireGuard Verbindungspartner verifiziert (14 Buchstaben):

8 waagerecht: Ausführungsbereich, in dem OpenVPN läuft, was Overhead durch Kontextwechsel verursacht (9 Buchstaben):

SENKRECHT

1 senkrecht: Geringe Größe der WireGuard-Codebasis, die die Prüfung deutlich erleichtert (13 Buchstaben):

3 senkrecht: Ausführungsbereich des Betriebssystems, in dem WireGuard für mehr Geschwindigkeit läuft (11 Buchstaben):

5 senkrecht: Modernes VPN-Protokoll für hohe Geschwindigkeit und einfache Code-Prüfung (9 Buchstaben):

6 senkrecht: Transportprotokolle, die OpenVPN unterstützt; WireGuard selbst läuft nur über eines davon (9 Buchstaben):

Kontrollpunkt 6: Suchsel

Finden Sie die 8 wichtigen Fachbegriffe, die im Gitter unten versteckt sind. Die Wörter können waagerecht, senkrecht oder diagonal verlaufen.

E K T S V R Z E H E S C A L Q
D C Z D R A U G E R I W M O T
O K V R O P E N S S L U P C A
C S W J M M H H N H R E P F K
R T L R W H B U F Y N U O Y W
E S H T X A P U N V N N Z O I
T Q T I P V U O P D U U K A E
K P M K A N V N U G G P Q X Y
A J K V J Y W D Y P J I Z I J
P N A E C A P S R E S U E I A
M S C H L U E S S E L P A A R
O S A J F W E K Z K E K Q N J
K A K E R N E L S P A C E F O
K N D N C D H I B A P R L P W
T I Y F Y S G X W H F R T N U

WORTSCHATZ-WORTLISTE

WIREGUARD OPENVPN KERNELSPACE USERSPACE KOMPAKTERCODE
OPENSSL SCHLUESSELPAAR TCPUNDUDP

Kontrollpunkt 6, Alternative: Barrierefreie Begriffszuordnung

Ordnen Sie jeden der 8 Fachbegriffe aus dem Suchrätsel der richtigen Definition zu, indem Sie den Buchstaben (A–H) in die Lücke schreiben.

FACHBEGRIFFE

- **A. WIREGUARD**
- **B. OPENVPN**
- **C. KERNELSPACE**
- **D. USERSPACE**
- **E. KOMPAKTERCODE**
- **F. OPENSSL**
- **G. SCHLUESSELPAAR**
- **H. TCPUNDUDP**

DEFINITIONEN UND ZUORDNUNGSFELDER

_____ 1. Kryptografische Bibliothek, auf deren Chiffrier-Algorithmen OpenVPN angewiesen ist.

_____ 2. Ausführungsbereich des Betriebssystems, in dem WireGuard für mehr Geschwindigkeit läuft.

_____ 3. Robustes, älteres Protokoll mit großer, komplexer Konfigurations-Codebasis.

_____ 4. Asymmetrische Token, mit denen WireGuard Verbindungspartner verifiziert.

_____ 5. Transportprotokolle, die OpenVPN unterstützt; WireGuard selbst läuft nur über eines davon.

_____ 6. Geringe Größe der WireGuard-Codebasis, die die Prüfung deutlich erleichtert.

_____ 7. Modernes VPN-Protokoll für hohe Geschwindigkeit und einfache Code-Prüfung.

_____ 8. Ausführungsbereich, in dem OpenVPN läuft, was Overhead durch Kontextwechsel verursacht.

Kontrollpunkt 7: Buchstabensalat

Bringen Sie die Buchstaben unten in die richtige Reihenfolge, um zentrale VPN-Begriffe aufzudecken. Schreiben Sie Ihre Antworten in die ausfüllbaren Eingabefelder.

1. UGEIWARDR
2. EEEKCLRAPSN
3. OKECRDEMTAKOP
4. CSALLEERSAPSHU
5. VNNEOPP
6. CRSAPUSEE
7. OSSLPNE
8. PNDTUCDUP

Bonusaufgabe: Schnell denken

3 ANTWORTEN PRO KATEGORIE. WER DIE LISTE ZUERST VOLLSTÄNDIG AUSFÜLLT, GEWINNT.

1	Gründe, sich für WireGuard zu entscheiden			
2	Versprechen, die ein guter VPN-Anbieter gibt			
3	Gründe, sich für OpenVPN zu entscheiden			
4	Gründe, auf Reisen ein VPN zu nutzen			
5	Dinge, die Ihr Internetanbieter sehen kann			
6	Möglichkeiten, ein gefälschtes WLAN zu erkennen			
7	Mythen über VPNs			
8	Orte, an denen Sie ein VPN nutzen würden			
9	Schnelle Dinge im Alltag			
10	Dinge, vor denen ein VPN Sie nicht schützen kann			
11	Dinge, die Code leichter überprüfbar machen			
12	Dinge, die ein VPN verbergen kann			
13	Unterschiede zwischen WireGuard und OpenVPN			
14	Wörter rund um Privatsphäre			
15	Namen von Verschlüsselungsverfahren, die Sie kennen			

Kontrollpunkt 8: Fallstudien zu VPNs

Wenden Sie die erlernten Konzepte an, um die folgenden praxisnahen Szenarien zu lösen.

SARAH (STUDENTIN IM CAFÉ)

👩‍💻 „Hallo! Ich bin im WLAN des Cafés, und meine VPN-App lässt mich zwischen WireGuard und OpenVPN wählen. Meine Videoanrufe brechen immer wieder ab, wenn ich zwischen dem Café-Netzwerk und dem Hotspot meines Handys wechsle. Welches Protokoll sollte ich wählen, und warum käme es mit dem Wechsel besser zurecht?“

ALEX (REISENDER STUDENT)

👩‍💻 „Ich bin im Ausland in einem Hotelnetzwerk, das offenbar den meisten VPN-Verkehr blockiert. WireGuard verbindet sich überhaupt nicht, aber ich muss auf die Ressourcen meiner Schule zu Hause zugreifen. Was wird wahrscheinlich blockiert, und wie könnte OpenVPN mir helfen, durchzukommen?“

Kontrollpunkt 9: Entschlüsselung der Chiffre

Um Ihr Training zur Protokollprüfung abzuschließen, entschlüsseln Sie diese versteckte Nachricht über die Ausführung im Kernel-Space.

SCHLÜSSEL FÜR DIE BUCHSTABEN-ZAHLEN-VERSCHLÜSSELUNG

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

18 21 5 19 20 5 14 19 9 5 22 15 14

15 16 5 14 22 16 14 1 21 6

19 3 8 14 5 12 12 5 18 5 20 21 14 14 5 12 21 13

Entschlüsselte Nachricht:

TIPP: JEDE ZAHL STEHT FÜR DIE POSITION DIESES BUCHSTABENS IM ALPHABET (Z. B. 1 = A, 2 = B, 26 = Z).

Kontrollpunkt 10: Grundlegende häufige Fragen zu VPN (Teil A)

Sehen Sie sich die häufigsten Fragen und Antworten an, die Interessenten zur Nutzung virtueller privater Netzwerke haben.

Q1: Was ist ein VPN und wie funktioniert es?

Ein Virtual Private Network (VPN) verschlüsselt Ihre Internetverbindung und leitet Ihren Datenverkehr über einen sicheren entfernten Server. Dadurch wird Ihre öffentliche IP-Adresse verschleiert, und es wird eingeschränkt, was Beobachter im lokalen Netzwerk und Ihr ISP über den durch den VPN-Tunnel geleiteten Datenverkehr sehen können.

Q2: Warum sind Protokolle wichtig?

Das Protokoll bestimmt, wie Ihr VPN seinen Tunnel aufbaut, welche Kryptografie Ihre Daten schützt und wie schnell es sich verbindet und neu verbindet. WireGuard und OpenVPN sind die beiden Open-Source-Protokolle, die die meisten VPN-Apps anbieten, und sie wägen Einfachheit, Geschwindigkeit und Konfigurierbarkeit unterschiedlich ab.

Q3: Ist einer der beiden privater als der andere?

Keines der beiden Protokolle macht Sie anonym. Beide verschlüsseln den Tunnelverkehr mit starken Chiffren; Ihre Privatsphäre hängt vor allem davon ab, was der VPN-Anbieter protokolliert und wie er Schlüssel, Konten und Server verwaltet.

Q4: Verlangsamt ein VPN meine Internetgeschwindigkeit?

Ja, leicht. Der Verschlüsselungsvorgang und die räumliche Entfernung zum VPN-Server erhöhen Latenz und Overhead. Die Auswirkung hängt von Anbieter, Protokoll, Serverentfernung, Gerät und Netzwerkbedingungen ab.

Q5: Sind beide Open Source?

Ja. WireGuard und die OpenVPN Community Edition veröffentlichen beide ihren Quellcode, sodass unabhängige Forscher ihn prüfen können. Durch die kleine Codebasis von WireGuard ist eine vollständige Prüfung deutlich schneller möglich.

Kontrollpunkt 10: Grundlegende häufige Fragen zu VPN (Teil B)

Sehen Sie sich die häufigsten Fragen und Antworten an, die Interessenten zur Nutzung virtueller privater Netzwerke haben.

Q6: Welches ist schneller?

WireGuard ist meist schneller: Es läuft im Kernel, nutzt die schlanke ChaCha20-Poly1305-Verschlüsselung und schließt Handshakes schnell ab. OpenVPN hat mehr Overhead, doch die tatsächlichen Geschwindigkeiten hängen auch von Serverauslastung und Entfernung ab.

Q7: Können beide über TCP und UDP laufen?

Nein. OpenVPN kann über UDP oder TCP laufen, und der TCP-Modus hilft in Netzwerken, die UDP blockieren. WireGuard sendet seine Pakete nur über UDP und kann daher in Netzwerken scheitern, die nur TCP zulassen. [4]

Q8: Wie wähle ich das beste VPN aus?

Achten Sie auf geprüfte No-Logs-Richtlinien, starke Protokolle (WireGuard, OpenVPN), sichere Serverstandorte, hohe Geschwindigkeiten, reine RAM-Server, eine Kill-Switch-Funktion und eine Rechtsordnung außerhalb von Geheimdienstallianzen (wie den 5/9/14 Eyes).

Q9: Kann ich WireGuard und OpenVPN auf meinem Smartphone verwenden?

Ja. WireGuard ist plattformübergreifend und bietet Apps für Windows, macOS, Linux, iOS und Android; OpenVPN-Clients gibt es für dieselben Systeme. In den meisten VPN-Apps können Sie eines der beiden auswählen. [1]

Q10: Warum ist WireGuard so klein?

WireGuard unterstützt einen festen Satz moderner Chiffren statt vieler Optionen. Seine Linux-Implementierung benötigt weniger als 4.000 Codezeilen und lässt sich daher leichter prüfen als umfangreichere VPN-Codebasen. [3]

Kontrollpunkt 10: Fortgeschrittene häufige Fragen zu VPN (Teil C)

Erkunden Sie technische und strukturelle Aspekte virtueller privater Netzwerke und sicherer Tunnelprotokolle.

Q1: Was ist der Unterschied zwischen WireGuard, OpenVPN und IKEv2?

WireGuard ist ein modernes, schlankes Protokoll (nur ca. 4.000 Codezeilen), das hohe Geschwindigkeiten und kurze Verbindungszeiten bietet. OpenVPN ist ein sehr sicheres, praxiserprobtes Open-Source-Protokoll. IKEv2 eignet sich hervorragend für Mobilgeräte, da es sich beim Netzwerkwechsel schnell wieder verbindet.

Q2: Welche Chiffren verwendet WireGuard?

WireGuard verwendet ChaCha20 mit Poly1305 zur Verschlüsselung, Curve25519 für den Schlüsselaustausch, BLAKE2s zum Hashing und das Noise-Framework für den Handshake. Es gibt keine Aushandlung von Chiffren, daher können Nutzer keine schwache Option wählen. [2]

Q3: Welche Chiffren und Bibliotheken kann OpenVPN verwenden?

OpenVPN ist eng mit der OpenSSL-Bibliothek verbunden und nutzt TLS für den Schlüsselaustausch. Administratoren können Chiffren für den Datenkanal wie AES-256-GCM wählen, was Flexibilität bietet, aber auch Raum für schwache Einstellungen lässt. [4]

Q4: Wie authentifiziert jedes Protokoll die Gegenstellen?

WireGuard-Peers identifizieren sich gegenseitig über statische öffentliche Schlüssel, ähnlich wie beim Austausch von SSH-Schlüsseln, und jeder Schlüssel ist zulässigen Tunnel-IPs zugeordnet. OpenVPN stützt sich meist auf eine Zertifizierungsstelle mit X.509-Zertifikaten, oft kombiniert mit Benutzername und Passwort.

Q5: Wie umgeht Verschleierung (Obfuscation) VPN-Sperren?

Verschleierung (oder „Stealth VPN“) tarnt VPN-Verkehr so, dass er wie gewöhnlicher HTTPS-Verkehr (Port 443) aussieht. Das kann helfen, die Deep Packet Inspection (DPI) zu umgehen, mit der Regierungen oder Schul- und Firmennetzwerke VPNs blockieren.

Kontrollpunkt 10: Fortgeschrittene häufige Fragen zu VPN (Teil D)

Erkunden Sie technische und strukturelle Aspekte virtueller privater Netzwerke und sicherer Tunnelprotokolle.

Q6: Was passiert, wenn ich vom WLAN zum Mobilfunknetz wechsle?

WireGuard ist verbindungslos: Es sendet Pakete von der neuen Adresse, und der Tunnel läuft nach einem kurzen Handshake weiter. OpenVPN speichert einen Sitzungsstatus, daher kann ein Netzwerkwechsel eine erneute Verbindung erfordern, die etwas länger dauert.

Q7: Wie funktioniert Forward Secrecy (Perfect Forward Secrecy)?

PFS stellt sicher, dass für jede einzelne Sitzung ein eigener, temporärer Schlüssel erzeugt wird. Selbst wenn ein privater Schlüssel künftig kompromittiert wird, kann er nicht zur Entschlüsselung vergangener oder zukünftiger Sitzungen genutzt werden, da diese unabhängige Schlüssel verwendeten.

Q8: Ist OpenVPN noch eine gute Wahl, wenn WireGuard schneller ist?

Ja. OpenVPN ist ausgereift und weit verbreitet, läuft über TCP, wenn UDP blockiert ist, und unterstützt zertifikatsbasierte Unternehmenskonfigurationen. Viele Anbieter bieten beide Protokolle an, damit Nutzer wechseln können, wenn eines blockiert oder langsam ist.

Q9: Welche Ports verwenden sie?

Der Standardport von OpenVPN ist 1194, er kann aber auf jeden UDP- oder TCP-Port verlegt werden, auch auf 443. WireGuard lauscht auf einem UDP-Port, der in seiner Konfiguration festgelegt wird; 51820 ist der Port aus den offiziellen Beispielen.

Q10: Welches Protokoll lässt sich leichter manuell einrichten?

WireGuard ist meist einfacher: Schlüsselpaar erzeugen, öffentliche Schlüssel austauschen und zulässige IPs eintragen. OpenVPN benötigt Zertifikate, eine CA und mehr Optionen, auch wenn .ovpn-Profile diese in einer Datei bündeln.

Teil 11: 10 interessante VPN-Fakten und Einblicke aus der Praxis

Lernen Sie diese besonders wertvollen, realen Fakten und Erkenntnisse zur Geschichte, zum Markt und zur Technologie von VPNs kennen.

1. ERSTES VPN-PROTOKOLL

PPTP (Point-to-Point Tunneling Protocol) wurde von einer Herstellergruppe unter Beteiligung von Microsoft entwickelt und im Juli 1999 als RFC 2637 veröffentlicht, um VPNs für den Fernzugriff zu unterstützen. [6]

2. ZWEI TRANSPORTWEGE

OpenVPN kann seinen Tunnel über UDP oder TCP übertragen, und im TLS-Modus teilen sich Steuer- und Datenkanal einen einzigen Port. [4]

3. WIREGUARD-REVOLUTION

WireGuard hat eine stark verschlankte, auf Effizienz ausgelegte Codebasis, die sich leichter auf Sicherheitslücken prüfen lässt als herkömmliche Protokolle. [3]

4. MODERNE KRYPTOGRAFIE

WireGuard kombiniert ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 und HKDF innerhalb des Noise-Protokoll-Frameworks, ohne Chiffre-Optionen, bei denen Nutzer etwas falsch einstellen könnten. [2]

5. OPENSSL IN OPENVPN

OpenVPN ist eng mit der OpenSSL-Bibliothek verbunden und bezieht viele seiner kryptografischen Fähigkeiten daraus, darunter das TLS für den Schlüsselaustausch. [4]

6. DEEP PACKET INSPECTION

Deep Packet Inspection (DPI) untersucht Paketinhalte und Verkehrsmuster, nicht nur Header, und einige Firewalls nutzen sie, um gängige VPN-Protokolle zu erkennen und zu blockieren.

7. SCHLÜSSEL IM SSH-STIL

WireGuard-Verbindungen werden durch den Austausch einfacher öffentlicher Schlüssel eingerichtet, ähnlich wie beim Austausch von SSH-Schlüsseln, ohne dass eine Zertifizierungsstelle nötig ist. [1]

8. PLATTFORMÜBERGREIFEND

WireGuard wurde zuerst für den Linux-Kernel veröffentlicht und ist heute für Windows, macOS, BSD, iOS und Android verfügbar, sodass dasselbe Protokoll auf den meisten Geräten funktioniert. [1]

9. FORWARD SECRECY

WireGuard wiederholt seinen Noise_IK-Handshake alle paar Minuten, um die symmetrischen Sitzungsschlüssel zu wechseln, und bietet so Perfect Forward Secrecy, selbst wenn ein langfristiger Schlüssel später bekannt wird. [2]

10. TUN/TAP-SCHNITTSTELLEN

OpenVPN ist für die virtuelle Netzwerkschnittstelle TUN/TAP ausgelegt, die auf den meisten Plattformen verfügbar ist und die Pakete des Tunnels überträgt. [4]

Technische Referenzen und Quellen

Zitierte Veröffentlichungen, kryptografische Spezifikationen und offizielle Dokumentstandards, die in diesem Arbeitsblatt verwendet werden.

WISSENSCHAFTLICHE UND FACHLICHE QUELLEN

[1] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.

https://www.wireguard.com/

[2] WireGuard. (n.d.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

[3] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.

https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.

https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] WireGuard. (n.d.). Quick Start.

https://www.wireguard.com/quickstart/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).

https://datatracker.ietf.org/doc/html/rfc2637

Lösungsschlüssel: Vergleich der Protokolle WireGuard und OpenVPN, ihrer Codebasisgrößen, Geschwindigkeit und kryptografischer Standards

1 **Codeumfang von WireGuard** PROTOKOLLE — **Richtige Antwort: D**

HINWEIS FÜR LEHRKRÄFTE

WireGuard ist äußerst kompakt und umfasst nur etwa 4.000 Codezeilen. Das hält die Angriffsfläche klein und erleichtert Audits. Quelle: WireGuard Project.

2 **Geschwindigkeit im Kernelbereich** LATENZ — **Richtige Antwort: B**

HINWEIS FÜR LEHRKRÄFTE

Da WireGuard direkt im Kernelbereich ausgeführt wird, vermeidet es den Overhead von Kontextwechseln und ermöglicht hohen Durchsatz. Quelle: WireGuard Project.

3 **Frage 3** — **Richtige Antwort: B**

HINWEIS FÜR LEHRKRÄFTE

OpenVPN ist eng mit OpenSSL verzahnt, das Verschlüsselungsverfahren wie AES-GCM bereitstellt; das macht es sehr flexibel konfigurierbar, aber auch komplexer.

4 **Protokollleistung** ROUTING-STEUERUNG — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

WireGuard baut Handshakes in Millisekunden auf und reagiert sofort auf Netzwerkwechsel (z. B. vom WLAN ins Mobilfunknetz). Quelle: Microsoft Native Gateway, Apple Support.

5 **Asymmetrische Kryptografie** PRIVATSPHÄRE — **Richtige Antwort: C**

HINWEIS FÜR LEHRKRÄFTE

WireGuard nutzt Cryptokey Routing und ordnet öffentliche Schlüssel zulässigen Tunnel-IP-Adressen zu, ähnlich wie bei SSH-Konfigurationen. Quelle: WireGuard Project.

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 Frage 6

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Die Linux-Implementierung von WireGuard umfasst weniger als 4.000 Zeilen, sodass Sicherheitsteams sie weit schneller prüfen können als viel größere VPN-Codebasen wie OpenVPN.

7 Latenz im User-Space GESCHWINDIGKEITEN

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

OpenVPN läuft im User-Space und reicht Pakete zwischen sich und der virtuellen Kernel-Schnittstelle hin und her, was zusätzlichen Overhead durch Kontextwechsel verursacht (sofern keine Kernel-Auslagerung wie OpenVPN DCO genutzt wird). Quelle: DD-WRT custom firmware.

8 OpenVPN-Konfiguration SNIFFING-RISIKO

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

OpenVPN kann über TCP (für Zuverlässigkeit/Umgehung von Firewalls) oder UDP (für Geschwindigkeit) laufen und ist daher mit komplexen Unternehmens-Firewalls kompatibel. Quelle: IETF Cryptographic Protocols.

9 Moderne Kryptografie FIREWALLS

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

WireGuard verzichtet auf veraltete Chiffren und setzt stattdessen auf moderne, sichere Primitive wie ChaCha20 und Poly1305, die auf mobilen CPUs schnell laufen. Quelle: WireGuard Project.

10 Vereinfachung durch Schlüsselpaare NO-LOGS

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

WireGuard verwendet keine Zertifikate oder komplexen CA-Hierarchien, sondern einfache Paare aus öffentlichen und privaten Schlüsseln, die zwischen den Peers ausgetauscht werden. Quelle: WireGuard Project.

Vokabelschlüssel und Bewertungsraster

Bewertungsraster für Lehrkräfte: Vergeben Sie 1 Punkt für jede richtige Zuordnung (insgesamt 8 Punkte) und jeden Kontextbegriff (insgesamt 6 Punkte).

KONTROLLPUNKT 4: LÖSUNG BEGRIFFSZUORDNUNG

G 1. WireGuard	H 2. OpenVPN	E 3. Kernel-Space	A 4. User-Space
B 5. 4.000 Zeilen	C 6. OpenSSL	F 7. Schlüsselpaar	D 8. TCP/UDP

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 WIREGUARD	2 OPENVPN	3 KERNEL SPACE	4 USER SPACE
5 SCHLÜSSELPAAR	6 PRÜFBARKEIT		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 F – OPENSSL	2 C – KERNELSPACE	3 B – OPENVPN	4 G – SCHLUESSELPAAR
5 H – TCPUNDUDP	6 E – KOMPAKTERCODE	7 A – WIREGUARD	8 D – USERSPACE

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden WireGuard, OpenVPN und Kernel-Space in eigenen Worten erklären und jeweils ein Beispiel nennen können.

Fallstudien:
Bitten Sie die Lernenden, ihre Empfehlungen mit Fakten aus dem Arbeitsblatt statt mit Vermutungen zu begründen.

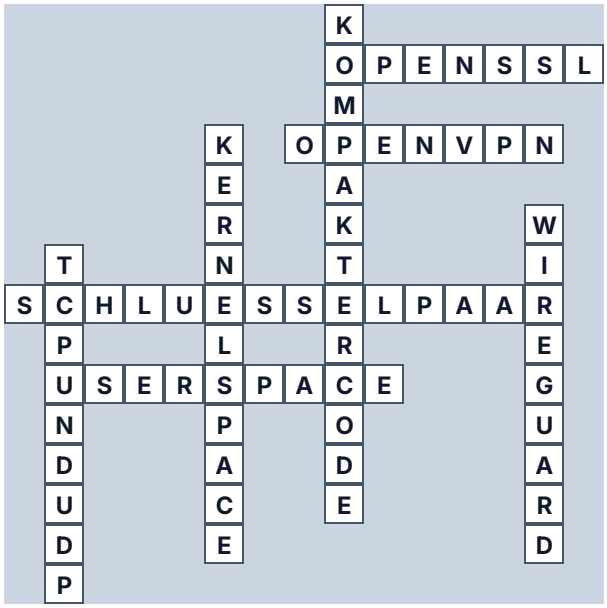
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS

E	K	T	S	V	R	Z	E	H	E	S	C	A	L	Q
D	C	Z	D	R	A	U	G	E	R	I	W	M	O	T
O	K	V	R	O	P	E	N	S	S	L	U	P	C	A
C	S	W	J	M	M	H	H	N	H	R	E	P	F	K
R	T	L	R	W	H	B	U	F	Y	N	U	O	Y	W
E	S	H	T	X	A	P	U	N	V	N	N	Z	O	I
T	Q	T	I	P	V	U	O	P	D	U	U	K	A	E
K	P	M	K	A	N	V	N	U	G	G	P	Q	X	Y
A	J	K	V	J	Y	W	D	Y	P	J	I	Z	I	J
P	N	A	E	C	A	P	S	R	E	S	U	E	I	A
M	S	C	H	L	U	E	S	S	E	L	P	A	A	R
O	S	A	J	F	W	E	K	Z	K	E	K	Q	N	J
K	A	K	E	R	N	E	L	S	P	A	C	E	F	O
K	N	D	N	C	D	H	I	B	A	P	R	L	P	W
T	I	Y	F	Y	S	G	X	W	H	F	R	T	N	U

KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

2 waagerecht: OPENSSL Kryptografische Bibliothek, auf deren Chiffrier-Algorithmen OpenVPN angewiesen ist (7 Buchstaben)

4 waagerecht: OPENVPN Robustes, älteres Protokoll mit großer, komplexer Konfigurations-Codebasis (7 Buchstaben)

7 waagerecht: SCHLUESSELPAAR Asymmetrische Token, mit denen WireGuard Verbindungspartner verifiziert (14 Buchstaben)

8 waagerecht: USERSPACE Ausführungsbereich, in dem OpenVPN läuft, was Overhead durch Kontextwechsel verursacht (9 Buchstaben)

SENKRECHT

1 senkrecht: KOMPAKTERCODE Geringe Größe der WireGuard-Codebasis, die die Prüfung deutlich erleichtert (13 Buchstaben)

3 senkrecht: KERNELSPACE Ausführungsbereich des Betriebssystems, in dem WireGuard für mehr Geschwindigkeit läuft (11 Buchstaben)

5 senkrecht: WIREGUARD Modernes VPN-Protokoll für hohe Geschwindigkeit und einfache Code-Prüfung (9 Buchstaben)

6 senkrecht: TCPUNDUDP Transportprotokolle, die OpenVPN unterstützt; WireGuard selbst läuft nur über eines davon (9 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

Lösungsschlüssel für die Wort-Entwirr-Aufgabe und die Geheime Chiffre-Aufgabe.

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. UGEIWARDR — **WIREGUARD**
2. EEEKCLRAPSN — **KERNELSPACE**
3. OKECRDEMTAKOP — **KOMPAKTERCODE**
4. CSALLEERSAPSHU — **SCHLUESSELPAAR**
5. VNNEOPP — **OPENVPN**
6. CRSAPUSEE — **USERSPACE**
7. OSSLPNE — **OPENSSL**
8. PNDTUCDUP — **TCPUNDUDP**

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"RUESTEN SIE VON OPENVPN AUF SCHNELLERE TUNNEL UM"

Lösungsschlüssel zu den Fallstudien

A Szenario A: Auswahl eines Protokolls

SNIFFING UND VERSCHLÜSSELUNG | Sarahs Dilemma

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Empfehlung: WireGuard. Sein schlankes, verbindungsloses Design lässt den Tunnel sich schnell erholen, wenn sich ihr Netzwerk ändert, und ChaCha20-Poly1305 hält die Verschlüsselung schnell.
- Sicherheit: Beide Protokolle verschlüsseln ihren Datenverkehr im Café-WLAN, sodass bei korrekter Konfiguration jedes davon ihre Anmeldungen schützt; die Wahl wirkt sich hauptsächlich auf Geschwindigkeit und Stabilität aus.

B Szenario B: VPN-Sperren überwinden

GEOBLOCKING UND IPS | Alex' Dilemma

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Warum blockiert: WireGuard nutzt ausschließlich UDP, und die Hotel-Firewall blockiert wahrscheinlich UDP oder erkennt WireGuard-Pakete durch Filterung oder Deep Packet Inspection.
- So hilft OpenVPN: Es kann über TCP laufen, auch über Port 443, den HTTPS nutzt und den Hotel-Firewalls selten komplett sperren, weil das Surfen im Web davon abhängt.